ELIT NET

Data Analytics Platform

Data analysis and anomaly detection for CSPs

Elitnet’s **Data Analytics Platform** (DAP) is a high-performance data analysis platform which covers data collection from multiple sources, AI/ML enabled data processing, and powerful reporting and monitoring tools.

The platform provides a set of built-in data processing applications/data processors (such as Fraud Prevention, DDoS Attack Detection, etc.) and is open for creation and deployment of new applications. The platform also provides a rich set of tools for data analytics.

To provide both excellent reliability and outstanding price performance, DAP uses a combination of open source and branded systems for data collection, storage, and processing. The platform provides CSPs with the following key values:

Fraud Prevention

Data Analytics Platform analyzes call detail records (CDRs) and identifies a wide range of fraudulent activities based on predefined rules as well as subscriber behavior analysis/learning and subscriber profile classification.

Traffic Classification

The platform can classify both encrypted and unencrypted traffic and provide it to other network infrastructure components to ensure quality of service (QoS) and enable charging according to traffic type.

Service Degradation Detection

The platform analyzes service data, measures quality of experience (QoE), and detects anomalies which indicate service degradation, allowing the CSP to predict service problems and prevent service downtime.

SS7 and Diameter Threat Detection

DAP addresses prominent mobile network vulnerabilities by using a rule-based approach to detect attempts to intercept personal subscriber data, take over devices, and disrupt service. Previously unknown threats are also addressed based on anomaly detection.

Denial of Service Prevention

DAP looks for anomalies in data traffic to detect possible distributed denial-of-service (DDoS) attacks, attempts to block access to base stations, and attempts to disconnect devices from the network.

Predictive Network Maintenance

Using its anomaly detection capabilities, the platform predicts faults in various network components (e.g. base stations) and forecasts necessary network infrastructure expansions due to insufficient capacity.

Malware Detection

The data processor uses both signature databases (Snort) and machine learning-based methods such as IP to DN and IP to IP activity classification to detect and prevent attempts to disseminate malware in the network.

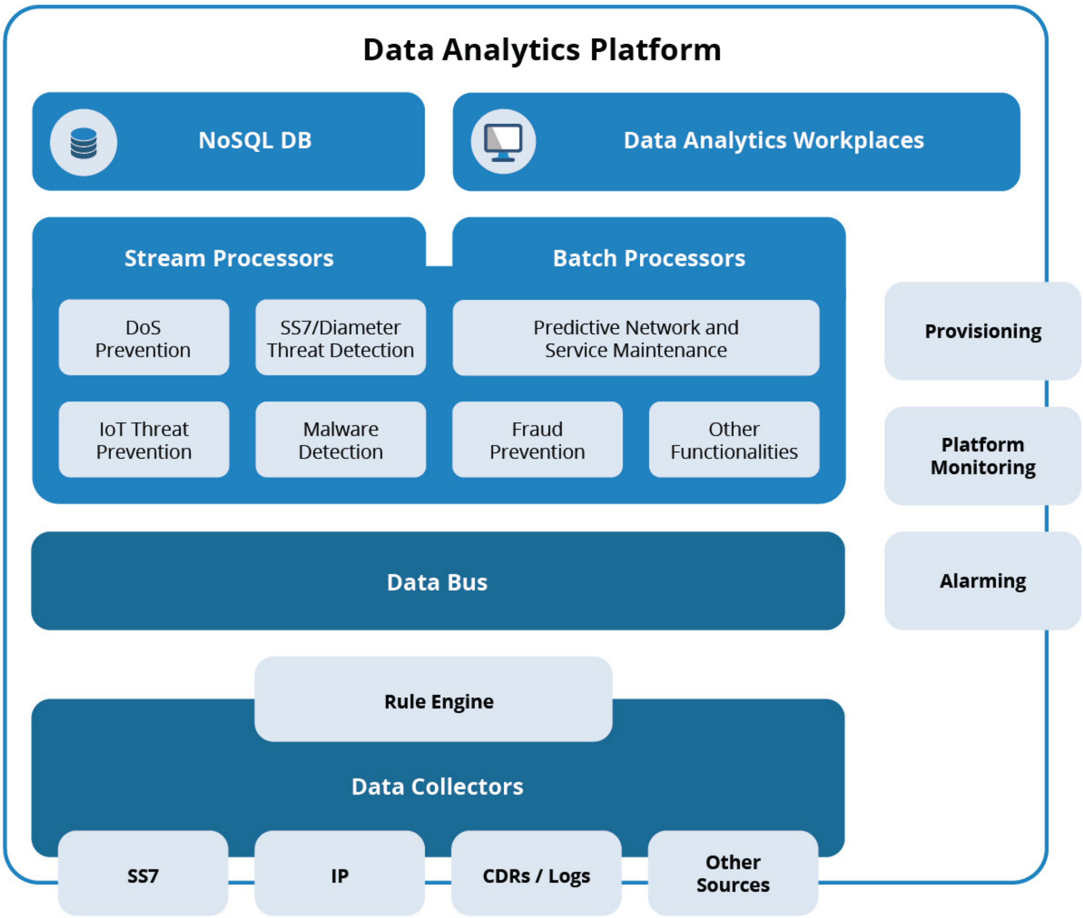
IoT Threat Prevention

DAP looks for anomalies in traffic related to IoT terminals to prevent any attacks on-network's IoT infrastructure and end-user devices. Real-time network monitoring enables instant anomaly detection.

The architecture of DAP is designed to ensure horizontal scalability, high availability, and zero downtime during maintenance, allowing the CSP to easily expand the platform's capacity without influencing its performance.

The key nodes of the platform include the **Data Collectors**, which collect network data from various sources, including SS7 traffic (via Dialogic Signaling Stack), real-time data traffic (via Napatech boards), CDRs, log files, and other sources. The data is then processed and pre-filtered by the Rule Engine and passed on to the **Data Bus** component using Apache Kafka open-source software.

The **Stream Processors** and **Batch Processors** analyze the data and search for any anomalies, while the **NoSQL Database** is used for large-volume data storage. The platform also contains Provisioning, Monitoring, and Alarming components which ensure flexible platform configuration and real-time performance monitoring.



Key Features and Functionalities

Elitnet's Data Analytics Platform encompasses the following main features and functionalities:

Graphical User Interface. DAP features a powerful graphical user interface (GUI) with the following featurs and functionalities: highly detailed data vizualization, fully customizable dashboards, data drilldown capability, flexible report builder, fully customizable alerts, and real-time alerting.

Passive Monitoring Mode. DAP works in monitoring mode and receives SS7 network data via mirror ports, ensuring no impact to normal network performance and security.

Data Aggregation. The platform aggregates data to reduce and prepare it for correct and comprehensive analysis.

Data Connectors. DAP uses data connector components to connect to various network resources and receive different types of data. The platform features the following data connectors:

- *SS7.* DAP utilizes the Dialogic Signaling Stack for integration with the SS7 network.
- *IP.* The platform uses a deep packet inspection component with Napatech boards to receive real-time data traffic from the IMS network.
- *Logs.* Additional data can be received from CDRs and network log files. The Data Bus component using Apache Kafka software can be used to easily integrate various data sources.

Proven Open Source Components. In addition to the reliable branded systems such as the Dialogic Signaling Stack, DAP uses a wide range of proven open source components which carry out various important tasks:

- *Aerospike* and *Cassandra* are used as the NoSQL Database components.
- *Apache Flink* is used for stream/batch processing.
- *Apache Kafka* is used as the Data Bus.
- *Grafana* and *Prometheus* are used for monitoring and alarming.
- *JasperReports* is used for report building

Diverse Anomaly Detection Methods. The platform uses a wide range of mathematical methods to analyze IP data, including IP fingerprint clustering, IP entropy analysis, HTTP request entropy analysis, and IPDN analysis.

Rule Engine. For higher data processing efectiveness, DAP includes a Rule Engine component which carries out data pre-filtering, discarding any unnecessary data and providing only relevant data to other components for analysis and anomaly detection. The Rule Engine also carries out the traffic classification functionality.

Horizontal Scalability. All DAP nodes are horizontally scalable, allowing the CSP to increase capacity by transparently adding additional nodes to the cluster. This ensures unlimited scale for the platform.

High Availability. The platform has no single point of failure and features high availability for all nodes, ensuring that the solution fully operates even in case one of the nodes fails.

Zero Downtime Maintenance. The platform ensures no downtime during regular and unplanned platform maintenance. Any nodes can be dynamically connected and disconnected without having any influence on system performance.

ELIT NET

www.elitnet.eu

info@elitnet.eu

+370 37 352706

UAB Elitnet
Pasiles 102, LT 51314
Kaunas, Lithuania